Legal Blackbook™

CyberInsecurity

JUNE 2018

WORKING WITH THE GOVERNMENT AFTER A BREACH

Four tips that companies should follow to maximize the benefits.

BY KIMBERLY PERETTI

The scope and frequency of security incidents continue to grow, as does the media and government attention to breaches. Different arms of the government continue to actively engage in this space, though they can have varying purposes and agendas. These range from investigating criminal actors behind security incidents, to providing threat intelligence, to sharing information with the broader public to enforcing violations of regulations and laws.

Some government agencies are eager to work with companies that have suffered breaches. This past January, FBI Director Christopher Wray said at a cybersecurity conference: "At the FBI, we treat victim companies as victims." Wray was encouraging companies to report cybercriminal activity and partner with his agency. But federal law enforcement is only one arm of government that a compromised entity may engage with after a data breach. Others have different mandates and goals.

As a company wades through the mass of decisions required when responding to a security event, it is important to understand in advance the different agencies that it may interact with. It's wise to be familiar with their agendas, which may or may not coordinate (to the benefit or detriment of the company), and what protections are available when providing them with sensitive and confidential information. Understanding these factors in advance, rather than during a live-fire incident (which many breach responses can be), will go many miles in helping a company navigate the full lifecycle of incident response.

A prime reason for victims to reach out to law enforcement is to gain valuable intelligence on the threat actors behind the intrusion.

Law Enforcement

Generally, law enforcement's primary function when they investigate cyber intrusions and data breaches is no different than when they investigate physical crimes: They gather evidence in order to identify, apprehend and prosecute criminals. Cyber crime is unique, however, in that digital evidence is particularly volatile, and cyber criminals can more easily obfuscate their identities and hide their tracks and behavior. Since a company's investigation often happens first and is more likely to preserve volatile data, law enforcement will often rely on shared information from

ALSTON & BIRD

victims rather than expend their own limited resources.

There are other differences as well. Law enforcement's role has evolved to include collecting and sharing threat intelligence with companies to help improve overall cyber defense. Since law enforcement gathers data about attackers from a number of different sources, they are often able to share the information that they learn both with victim companies experiencing a breach and through publicized alerts. This evolution is a significant development in the short history of cyber crime, and its importance cannot be overstated. A prime reason for victims to reach out to law enforcement is to gain valuable intelligence on the threat actors behind the intrusion.

Law enforcement also addresses national security investigations, especially as state-sponsored cyber attackers blur the line between traditional criminal and national security incidents. In contrast to a criminal investigation, a national security investigation's primary focus is often on gathering intelligence about a threat actor. Rather than press for an indictment, law enforcement may seek the most recently available indicators of compromise for an attacker, which can better identify and mitigate attacks. Other national security goals of a cyber investigation may include disrupting the infrastructure used by the actors, which often involves partnering with the private sector.

It's important to remember that there are many different branches of law enforcement, including state, local and federal agencies. Each has its own jurisdictional boundaries and may have limitations (resources or otherwise) that factor into whether it would be an appropriate entity to investigate any particular cyber crime. The Department of Justice's Computer Crime and Intellectual Property Section provides a chart to help companies identify which law enforcement entities to contact, depending on the type of incident.

Other Government Authorities

A company must be prepared not only to understand the nuances of working with law enforcement in the aftermath of a breach, but also to work with other arms of the government that are likely to become involved, particularly if an incident becomes public (e.g., through formal legal notification, popular press or other means). Two groups of government authorities in particular come to mind.

First is the Department of Homeland Security (DHS), which serves as a kind of cyber intelligence information clearinghouse. Whether through the U.S. Computer Emergency Readiness Team or through partnership with law enforcement or regulatory entities, DHS receives and collects cyber threat intelligence that it then shares with the rest of the public and government. Under the authority of the Cybersecurity Information Sharing Act, DHS, through the department's National Cybersecurity and Communications Integration Center, maintains the Automated Indicator Sharing portal for receiving and sharing cyber threat indicators with participating companies. Note, however, that the goal of this program is to share as many indicators as quickly as possible, so DHS does not validate those shared through the portal. When possible, though, DHS does assign a reputation score to specific indicators.

A company must be prepared not only to understand the nuances of working with law enforcement in the aftermath of a breach, but also to work with other arms of the government that are likely to become involved.

Second, and of course on the mind of any company in the midst of a breach response, are regulatory agencies. In contrast to law enforcement, regulators generally are most focused on protecting consumers. They also have, as a primary agenda item, compliance with applicable laws and regulations. On the federal level, there are both general and industry-specific regulators, including some with overlapping jurisdictions. For example, state attorneys general and the Federal Trade Commission (FTC) have general oversight authority and similar/overlapping jurisdiction. Since any individual incident can result in inquiries from one or more of these regulators, it is important for companies to know which regulators may investigate them and how to coordinate any such investigations.

The FTC actively investigates security incidents under its Section 5 enforcement powers to determine whether companies' security practices were deceptive or unfair to consumers. State attorneys general receive breach notifications and may publicly post information about incidents, up to and including the full notices themselves. One or more attorneys general may also conduct their own investigations into a breached company's practices, up to and including bringing cases and seeking fines for failure to comply with state and federal laws.

In contrast, the Department of Health and Human Services' Office of Civil Rights reviews and investigates notices from breached entities and complaints from consumers and conducts regular audits of HIPAA-regulated entities. Both the FTC and state AGs can similarly investigate incidents involving HIPAA or health-related information. These are good examples of overlapping jurisdictions on both the state and federal levels.

For companies to assess how to coordinate a multitude of regulatory investigations, it is important to understand overlapping jurisdictions and which agencies may not share information or coordinate in the wake of a breach. Knowing that law enforcement and regulators do not operate as "one united government" and rarely exchange information among themselves in the wake of an incident is often relevant in deciding whether to report to law enforcement. Indeed, this has been a long-standing concern of companies, and even prompted FBI Director Wray in March to reiterate that the FBI treats victims as victims, and that the FBI does not believe that it has a responsibility, after companies provide it with information, "to turn around and share that information with some of those other agencies."

ALSTON & BIRD

PRACTICE TIPS

Since involvement with government authorities is more a "when, not if" question, it is important for companies to plan for those interactions before an incident occurs. Below are four tips they should consider when anticipating working with the government.

1) Establish an Early Relationship

The better the communication between a company and the government after a security incident, the more likely that the relationship will be positive for both parties. With that in mind, the Department of Justice recommends establishing relationships with law enforcement before an incident occurs. Opening lines of communication before a data breach allows faster and clearer communication between the parties in a crisis.

2) Understand Each Arm of the Government's Purpose and Agenda

Understanding the purposes and agendas of different arms of the government can inform the company's interactions with them. The facts of the particular incident will influence both which agencies become involved and what goals those agencies will pursue. Anticipating those agendas can help a company prepare better communication and response plans.

3) Understand the Different Options and Protections for Sharing Information With the Government

When working with the government, companies have a variety of methods for sharing information. For federal law enforcement conducting a criminal investigation, companies may want to request a formal legal process before sharing information that has privacy implications. Information that a company shares with law enforcement is protected under the Federal Rules of Criminal Procedure when provided pursuant to a grand jury subpoena, for example. Sharing information this way can also avoid potential conflicts with the Electronic Communications Privacy Act and demonstrate a general commitment to the privacy of the individuals whose personal information the company holds. Recall also Wray's reminder that, at least in the eyes of the FBI, information shared with law enforcement need not be passed along to regulators.

Companies that do share information with regulators should consider exploring whether an applicable Freedom of Information Act exemption is possible. An exemption can mitigate the risk that sensitive data shared with a regulator will become public knowledge.

4) Understand How to Have a Coordinated Approach to Working With Different Arms of the Government

Since the various arms of government often have overlapping authorities and agendas, it is important to coordinate communications with them. Wherever possible, a company subject to multiple inquiries from different arms of the government, in particular various state and federal regulatory agencies, should identify whether a coordinated response is possible and in its interest. A well-coordinated response will incorporate all of the previous points to maximize the benefit to the company while minimizing the risks.

Kimberly Peretti *is a partner and co-chair of Alston & Bird's Cybersecurity Preparedness and Response Team and National Security and Digital Crimes Team. She is the former director of PwC's cyber forensic services group and a former senior litigator for the U.S. Department of Justice's Computer Crime and Intellectual Property Section. She draws on her background as both an information security professional and a lawyer in managing technical cyber investigations, assisting clients in responding to data security-related regulator inquiries, and advising boards and senior executives in matters of cybersecurity and risk. Peretti is a Certified Information Systems Security Professional (CISSP).*